PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown)

+1 Hotlists (2) Mark as Duplicate

Comments (7) Dependencies (0) Duplicates (0) Blocking (0) Resources (13)

Assigned Customer Issue P4 + Add Hotlist

STATUS UPDATE No update yet.

DESCRIPTION bu...@google.com created issue on behalf of György Istókovics #1 Aug 26, 2026 04:07AM

Summary: PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown)

Program: Google VRP

Vulnerability type: Sensitive data exposure

Details

PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown) Most people assume that when they hit the Delete button in Google AI Studio or Google Drive—and subsequently Empty the Trash—their data, prompts, and chat sessions are permanently destroyed.

This is factually false. I have proven on video through reproducible technical tests what actually happens behind the scenes.

:magnifying_glass_tilted_left: 1. The Core Architectural Difference: The JSON is a POINTER, the Prompt is the OBJECT Many misunderstand how this works, but here is the technical reality:

The JSON file on Google Drive: This is NOT the chat itself; it is merely a POINTER containing internal metadata, identifiers, and reference keys. The Prompt / Chat Session: This is the SERVER-SIDE OBJECT residing in Google's cloud infrastructure and backend databases. :collision: 2. The Experiment That Exposes the Architecture: Manual Re-upload (FAILS TO RESTORE): If you manually upload a previously downloaded .json prompt file back to Google Drive, the chat will NOT work or resume in AI Studio. Why? Because manual file upload generates new Drive file metadata and a new internal resource ID. Since the pointer is altered, AI Studio fails to bind it to the server-side object. Google Drive File Recovery (RESTORES IMMEDIATELY): When running the official Google Drive File Recovery tool on a "permanently deleted and trash-emptied" account: The recovery process restores the exact JSON file. The internal file metadata, resource IDs, and keys remain 100% identical to the original. Refreshing

Reporter	istokovicsgyorgy79@gmail.com
Type	Customer Issue
Priority	P4
Severity	S4
Status	Assigned
Access	Default access View
Expanded Access	
Assignee	wo...@google.com
Verifier	
Collaborators	
CC	istokovicsgyorgy79@gmail.com wo...@google.com Un-CC me
Code Changes	--
Pending Code Changes	--
Disclosure information	--

Google AI Studio immediately resurrects the entire chat—down to the exact prompt tokens, model parameters, and conversational context—fully functional and continuable! :brain: 3. The Irrefutable Technical Conclusion: If Google had genuinely destroyed the file or the chat from storage, the internal metadata would have changed upon recreation, rendering the chat permanently defunct.

Google never deleted the JSON file: It merely flagged it as hidden from the UI (Soft Delete / Hidden Flag). Google never deleted the server-side Prompt object: The conversation history and live model state remained fully intact in the backend. The “recovery tool” doesn’t reconstruct data from scratch: It simply reverts the hidden flag (unhide). Because the pointer metadata was never destroyed, the live chat resumes seamlessly. Summary: For the end user, “Deleting” and “Emptying the Trash” is just a visual illusion in the UI. Within Google’s backend architecture, both the JSON pointer and the underlying Prompt object remain fully preserved and active.

Here are the videos showing it, on PC and Android:

https://youtu.be/LBQfNbPCxQw

https://youtu.be/m4U6ajKuLRo

If Google’s server genuinely received a “delete / start countdown” command when I press the button, the server would immediately block access to the chat. If I restore the JSON pointer in Drive using a recovery bot and try to open the chat, in a real deletion system the server should say: “Hey, I see your key, but this chat is already marked for deletion in my system, I won’t load it!”

Since the chat loads immediately and perfectly, this can only mean one thing: Google’s server (the backend) never received any notification whatsoever that I clicked the delete button!

This is not “delayed deletion” and it is not a “grace period”. This is a classic case of “Orphaned Data”, intentionally built into the system.

The “Delete” button on the UI literally does NOTHING ELSE than moving the shortcut (JSON) in Drive to the trash. The AI model running on the server and the database have no clue about this; the data remains stuck there permanently (in an orphan state) without any deletion command ever being executed on it.

Since the server never even received the deletion command, it does not matter at all whether we wait 1 minute, 30 days, or 10 years. From the server’s perspective, the chat is alive and kicking; the user simply “lost” the map leading to it (the JSON). As soon as the map is restored (by the File Recovery tool), the path is open once again, as if nothing had happened.

I used the limitations of Google’s own File Recovery bot (the fact that it only accesses Drive and not the server) to expose the deception. With this, I have proven in black and white that Google AI Studio’s “Delete” button is a visual lie that makes the user believe data is being deleted from the server, while it never even touches the backend.

https://archive.ph/9kMHc

https://archive.ph/9kMHc/image

Attack scenario

Reporter e-mail	--
Requested charity	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

The “Delete” button on the UI literally does NOTHING ELSE than moving the shortcut (JSON) in Drive to the trash. The AI model running on the server and the database have no clue about this; the data remains stuck there permanently (in an orphan state) without any deletion command ever being executed on it.

Report Analysis

> **Note**: The feedback below was generated as part of an automated analysis of the submitted report. It is *NOT* part of the report that was submitted by the user.

Intended Behavior

The reported behavior appears to be intended. Please check the documentation.

Invalid Report

The report appears to match one of our common invalid report types.

COMMENTS

All comments ▾ | ↓ Oldest first

sp...@google.com <sp...@google.com> #2 Aug 26, 2026 04:07AM ⋮

NOTE: This is an automatically generated email

Hi! Many thanks for sharing your report.

This email confirms we've received your message. We'll investigate the issue you've reported and get back to you once we have an update. In the meantime, you might want to take a look at the list of frequently asked questions about Google Bug Hunters.

Also, if you have not already done so, create a profile on the Google Bughunters site if you'd like us to publicly recognize your contribution:

- Leaderboard – You'll be added here if we issue a reward for your report.
- Honorable Mentions – You'll be added here if you are not in the Hall of Fame, but we file a security vulnerability bug based on your report.

Note that we only act on reports concerning vulnerabilities or technical security problems in one of our products. This is not the correct channel if you need to resolve a problem with your account, or want to report non-security bugs or suggest a new product feature.

Cheers,
Google Security Bot

Follow us on Twitter!

sp...@google.com <sp...@google.com> #3 Aug 26, 2026 04:09AM

Status: Won't Fix (Intended Behavior).

Hi! We've reviewed your submission regarding data deletion in Google AI Studio and Google Drive. Although it may seem surprising, the behavior you're describing, where you can recover your own supposedly deleted chat data via Google Drive File Recovery, is actually working as intended from a security VRP perspective.

Our VRP rules on 'Intended Functionality' and 'Non-sensitive information disclosure' clarify that demonstrating the ability for a user to access or recover their *own* data, especially when they previously had access to it, is generally not considered a security vulnerability. This applies even if the data persists on our backend systems in a way that allows for recovery by the legitimate owner. For more context, you can refer to our VRP rules on the Google and Alphabet Vulnerability Reward Program and AI Vulnerability Reward Program, specifically the sections on 'Intended Functionality' and 'Prior Access' in the Non-sensitive information disclosure article.

If you think we've misunderstood your report, and you can show a well-defined security risk where an *unauthorized* third party gains access to data they shouldn't, please let us know what we missed.

Thanks again for your report and time,
The Google Bug Hunter Team

György Istókovics <istokovicsgyorgy79@gmail.com> #4 Aug 26, 2026 11:51AM

Subject: Re: Issue 552682596: PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown)
Dear Google Security & VRP Team,
Thank you for your review and for formally documenting the internal operating behavior of Google's backend infrastructure regarding Issue 552682596.
I take formal note of your written admission:
„This applies even if the data persists on our backend systems in a way that allows for recovery by the legitimate owner."
While your team evaluates this as "Intended Behavior" strictly from an internal VRP bounty eligibility scope, under European Union law—specifically GDPR Article 17 (Right to Erasure / Right to be Forgotten)—data controllers are legally mandated to permanently destroy personal data upon deletion request, rather than maintaining persistent backend states or orphaned interaction chains.

The fact that user prompts and full conversational contexts remain fully intact and restorable on your backend infrastructure after explicit deletion and trash emptying constitutes a direct, structural violation of European data protection regulations. The argument that "only the legitimate owner can recover it" is legally void under GDPR Article 17, which governs the absolute cessation of data processing and storage, not merely internal access restriction.
Please be advised that this case is now escalating to formal civil legal proceedings against Google LLC.
Your written confirmation, alongside the full video forensic evidence and technical documentation, has already been officially submitted to NOYB (European Center for Digital Rights) and is being directly integrated into the evidence package for upcoming civil litigation against Google LLC.
This matter will now be pursued and resolved directly in court and through specialized legal channels.
Sincerely,
György Istókovics (Bitu79)
istokovicsgyorgy79@gmail.com

<buganizer-system@google.com> ezt írta (időpont: 2026. aug. 26., Sze 4:10):

- Show quoted text -

György Istókovics <istokovicsgyorgy79@gmail.com> #5 Aug 26, 2026 12:29PM

Subject: Re: Issue 552682596: PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown)

Dear Google Security & VRP Team,

I would like to formally thank your team for your explicit, written confession regarding Google's backend data retention architecture.

By officially confirming that this system architecture is "working as intended" and that user data actively "persists on our backend systems" long after a user executes a permanent deletion request and empties their trash bin, you have provided the exact evidentiary foundation required to prove systematic, intentional data fraud.

Your internal security VRP scope cannot override or circumvent European Union law. Under GDPR Article 17, a permanent deletion request mandates the complete destruction of data on active production systems, not the creation of an invisible server-side cache that remains permanently harvestable via decoupled interaction links.

Thank you for handing over the "smoking gun" and documenting your own non-compliance so clearly in this ticket. Your written admission has been added as the primary exhibit to the legal filings.

See you in court.

Sincerely, György Istókovics (Bitu79) istokovicsgyorgy79@gmail.com

---

kl...@google.com <kl...@google.com> Aug 26, 2026 03:09PM

Status: Assigned (reopened).

György Istókovics <istokovicsgyorgy79@gmail.com> #6 Aug 26, 2026 03:43PM

Subject: Re: Issue 552682596: PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown)

Dear Google Security & Legal Team,

I take note of your sudden internal status change from "Intended Behavior" to "Assigned."

However, modifying the ticket status under pressure does not erase the fact that your team has already formally admitted in writing that Google actively retains deleted user data on its backend infrastructure. The systematic GDPR Article 17 violation has already been fully executed and forensically documented.

My 14-day legal deadline sent to the Google Ireland DPO remains active. You have two options to resolve this matter: either Google initiates a formal pre-trial settlement discussion immediately to compensate for this severe data fraud, or I will proceed directly with filing the civil lawsuit in court alongside NOYB.

If you wish to settle this outside of court, have your Legal Department contact me before the 14-day deadline expires. Otherwise, see you in front of the judge.

Sincerely,
György Istókovics (Bitu79)
istokovicsgyorgy79@gmail.com

<buganizer-system@google.com> ezt írta (időpont: 2026. aug. 26., Sze 15:09):

- Show quoted text -

György Istókovics <istokovicsgyorgy79@gmail.com> #7 Aug 26, 2026 04:59PM

Subject: Re: Issue 552682596: PROOF: Google AI Studio & Google Drive NEVER Actually Delete Your Chats! (Technical Breakdown)

Dear Google Security, Engineering, and Legal Team,

I take note of your sudden internal status change to "Assigned" and the involvement of engineer wo...@google.com.

However, let me make one thing absolutely clear: your sudden "damage control" and panic-driven patching attempts under pressure change nothing regarding the core of this case. In court, late regret is not an excuse—it is merely an aggravating circumstance.

Your recent scramble to work on the system serves as two definitive proofs:

1. The "Fix" is an Admission of Guilt: By suddenly rushing to patch the system, you are indirectly admitting that what your team previously defended in writing as a feature ("Intended Behavior" in Comment #3) was actually a severe, illegal, and GDPR-non-compliant architectural flaw. If it wasn't a violation, you wouldn't be desperately trying to fix it right now. This destroys the credibility of your previous official VRP stance.

2. The Violation Has Already Occurred: A structural violation of GDPR Article 17 does not retroactively disappear the moment you start patching the source code. The fact remains that for months—despite my repeated warnings and recorded certified mail sent to you since May—Google actively, knowingly, and illegally retained deleted user data on its backend infrastructure. The court does not judge what you are trying to clean up today; it judges the systematic data fraud you have actively executed and maintained for months.

Your official Comment #3 stating this retention was "working as intended" remains the ultimate "Smoking Gun" and is safely preserved across global public archives. Trying to change the ticket status now is just pathetic squirming.

The 14-day legal ultimatum sent to the Google Ireland DPO is ticking. You either initiate a formal pre-trial settlement immediately to compensate for this severe data fraud, or we resolve this directly in front of the judge.

Sincerely,
György Istókovics (Bitu79)
istokovicsgyorgy79@gmail.com

<buganizer-system@google.com> ezt írta (időpont: 2026. aug. 26., Sze, 15:09):

- Show quoted text -